Attacks on Facebook: Public Awareness, Actions and Prevention

Angha Baikar
Research Scholar, MCA
Thakur Institute of ManagementStudies, Career Development andResearch (TIMSCDR) Mumbai, India

Sanketkumar Dave
Research Scholar, MCA
Thakur Institute of ManagementStudies, Career Development andResearch (TIMSCDR) Mumbai, India

Vinita Gaikwad
Ph.D
Research Scholar, MCA
Thakur Institute of ManagementStudies, Career Development andResearch (TIMSCDR) Mumbai, India

ABSTRACT
Social networking websites such as Facebook, Twitter, Myspace, Google+, and LinkedIn are the popular social sites. Facebook is the most popular social networking site. Facebook is the most common platform to communicate with their other friends, family and share thoughts, photos, videos and lots of information. That is why Facebook has become a platform for cybercriminals and cybercrime. cybercriminals exploit sensitive and personal information through social engineering and reverse social engineering. Users are unaware of the privacy risks involved when they share their sensitive information on the social network sites. How to keep social networking sites more secure and more private are the challenges that have been a concern for every user.

Keywords
Social system protection issues, security issues, default protection setting protection mindfulness, interpersonal interaction destinations.

1. INTRODUCTION
Cyber is a typical term utilized for the computers interconnected as a part of a system. The quantity of clients in the system has expanded which brings in the concept called "Cybersecurity". Cyber security is characterized as providing security of the information on the cloud data server from robbery, harm or unapproved access. Presently the inquiries emerge from where the greatest security breach has occuredto th system. The more equivocal is the clients, the more their interest of getting to the data some may do intentionally and some accidentally, from this actualities clearly our psyche will float towards the long range informal communication destinations. "Long range interpersonal communication destinations" is an online medium that permits clients from various foundation to make a profile and connect with alternate clients on similar sites. Person to person communication locales, for example, Facebook, Myspace, Twitter and so forth have turned out to be so prevalent among the general population that they have begun to share each and every snapshot of their lives on these destinations. Long range interpersonal communication destinations are one of the most effortless types of correspondence nowadays and have turned into an unavoidable thing for youth. Each division of the general public is subject to these. In any case, social destinations have negative viewpoints too. In light of the developing ubiquity of these locales, they serve as an objective for cybercrime and assaults. It is for the most part in light of how clients are utilizing these locales like Facebook and some more. Assailants can without much of a stretch get to and assemble their own and delicate data. Clients are less mindful and slightest worried about the security setting. Also, they effectively get to be a casualty of protection and personality rupture. The absence of Cyberlearning is the fundamental driver of most important truths because of which private photographs and individual data are shared among the system. In this paper, our primary concern is towards how to overcome the security issues of Facebook. To examine and translate information from every one of the perspectives and conclusion of vague clients from a particular instructive foundation. The goal of recognizing defenselessness with protection and security framework is to assistance to control web wrongdoings connected with security and character rupture on Facebook. Furthermore, it expects to enhance default security arrangement of person to person communication locales Facebook.

2. LITERATURRE'REVIEW
The enthusiasm of social locales has been expanded and numerous papers have reviewed and distributed. Some of them talked about the security issues of long range informal communication locales, highlighting the dangers that cybercrime in taleswith online interpersonal interaction sites. Chewae. [1] concentrated on how individual data is being influenced by web and web-based social networking, furthermore talked about how the protection turn into a hazard and how to appoint security attention to avert security rupture. They highlighted the present circumstance on utilizing informal community and dangers that can influence the clients. At last they expressed some security mindfulness that can be rehearsed to be more mindful of informal organization threats.Gangopdhyay and Dhar [7] have distributed a report in which they have said that Social locales draw in youngsters and permit them chances to coexist with known and obscure individuals. Making companions with obscure individuals and adding them to their companions rundown may be considered as tasteful or as things that can be flaunted. So they concentrated on how and to what degree the revealing of individual data by clients is secure. They additionally engaged the security setting made by the person to person communication destinations like Facebook, Myspace Orkut, twitter and so on. The analysts Gunatilaka et al. [8] have published a report in which they have said that due to the expanding prominence of long range informal communication locales, clients have turned into an objective for assailants. Long range informal communication locales are based no social relationship among individuals. The general population share most extreme number of their own and delicate data in their social locales. On account of the individual data and simple availability, assailant is following clients to start with them to play out a few activities. Numerous locales ndeavored

to evade those abuses, however aggressors are still ready to defeat those efforts to establish safety. They likewise contains the issues incorporates a study on various protection and security issues in social locales. The issues finish up rotection hazard, character take, physical dangers, and hacking, hishing, spamming and malware assaults. Pesce and Casas [9] demonstrated that person to person communication clients purposely and unconsciously post certain sorts of private and delicate data that can bring about tremendous harm, hurt them. Shared news, photographs, recordings, private data and each development of genuine exercises with family and companions are worry of client security. They likewise attempted mindful clients the epochal breaks of their security and educate them the make of new protection safeguarding setting of labeling photographs on social locales. Krishnamurthy and Wills characterized and measured different security angles crosswise over various SNSs utilizing the idea of bits of shared data. They likewise uncovered that, much like conventional sites, outsider spaces track client's exercises in Social Networking Sites. In opposition to across the board suppositions. Boyd and Hargittai [10] specified that young person couldn't care less about security settings in social locales like Facebook. Leitch and Warren told in his a report; individual data can be procured by anyone whenever and at wherever through web. The have permitted clients to rub in a flash post their sentiments, share experience and a great deal all the more fascinating. Be that as it may, there are numerous issues in regards to security inside its surroundings. They investigated a few security vulnerabilities and dangers connected with Facebook. F. Stutzman and J. Kramer-Duffield provide guidance on the most proficient method to upgrade the security of clients in person to person communication locales. To stay away from fraud, they recommend making clients profiles private for companions just, which will decrease the data burglary hazards on Social Networking destinations. A. Verma et al. proposed a decentralized and circulated engineering that jelly protection and security of the clients in person to person communication locales. They improved the protection and security by the utilization of a cryptographic system like (Random Sequence Algorithm) RSA and Cyber signature. C. Marcum et al.suggested that clients may not comprehend the dangers connected with sharing individual data or the probability to utilize this information to anticipate profoundly secret information like government disability numbers. Yabing Liu, et al., (2011) attempted to enhance defaults and give better devices to looks after protection. In any case, they regretted that the full degree of protection issue stayed obscure and there was little measurement of the rate of off base security settings or the challenges clients confront while dealing with their security.

3. METHODOLOGY OF THE STUDY

This investigation of the exploration utilized poll based study technique. A point by point and all around organized survey were outlined and dispersed to the general population of a various foundation. This review was directed and the research was conducted based on the research done at the bellow mentioned university.

JamiaHamdard, Hamdard University, New Delhi.

JamiaMillia University, New Delhi

4. RESULTS AND DISCUSSION

The point of the examination is to concentrate on the issues and difficulties client confront while utilizing person to person communication destinations. Thus, the goal here is to break down and recognize powerlessness in security setting and to assess the hazard connected with character and protection rupture. So to study this, gather the factual information by directing a study among the distinctive clients having diverse foundation i.e. (understudy, workers, businessperson etc.).This poll comprises of 20 inquiries and a sum of 170 long range interpersonal communication clients was incorporated into the study. Distinctive clients have diverse supposition and the distinctive level of use. Firstly, get some information about their instruction level among them 70(41.18%) are postgraduate, 2.94% had studied Standard 10, while there were 16 clients (9.41) was in middle class, 50 individuals (29.41%) who had finished their under-graduation and 24 clients (14.18%) were holding a Graduate and 70 client (41.18%) were holding a Postgraduate and 2.94% client in doctorate. Alongside the training, level asked of their occupation i.e. their working status among them greatest number of clients were understudies i.e. 92%, while 2.35% was agent, and Govt. (1.76%), not Govt. (3.53%). This implies the most extreme number of clients were between the ages of 15 - 25 years.

4.1 Facebook Users

An aggregate 153(90%) clients out of 170 were to be discovered Facebook client and 10% clients were not having account on Facebook. Implies Facebook is entirely famous among individuals.

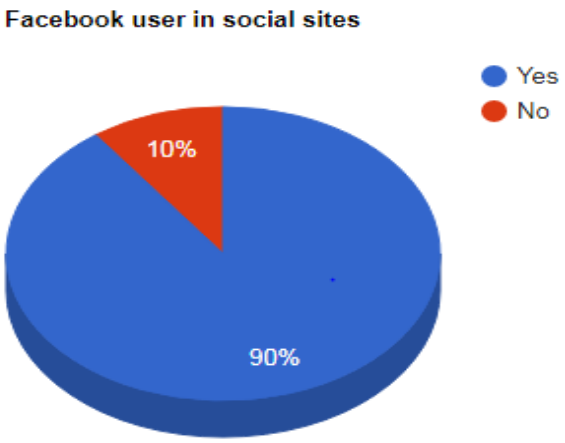

Fig 1: Pie chart of Facebook users in social networking sites

4.2 Using Other Social Networking Sites Status

There are diverse sorts of long range interpersonal communication locales, which were utilized as a part of the study.

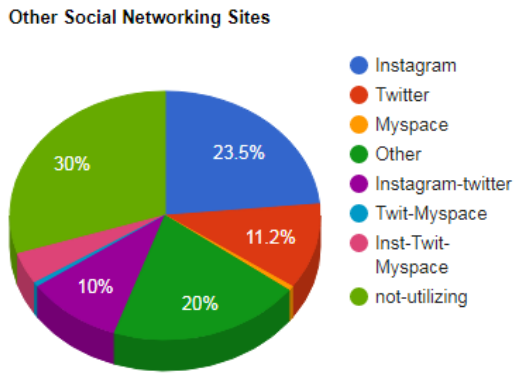

Fig 2: Pie chart of users are using other social networking sites

4.3 History of utilizing informal organization locales Duration

Bigger part of the 170 respondents, 53 customers (i.e. 31.18%) were using the Facebook for more than 5 years while minimum number (3.52%) of customer were using Facebook since one year and 5.29% customers were using from under 1 year, 8.23% of customers was using for more than 2 years, 10.59% of customers were using for more than 3 years, 15.88% of customers were using more than 4 years, however 15.29% of customers were using the Facebook for under 5 years, and 10% of customers were not using Facebook.

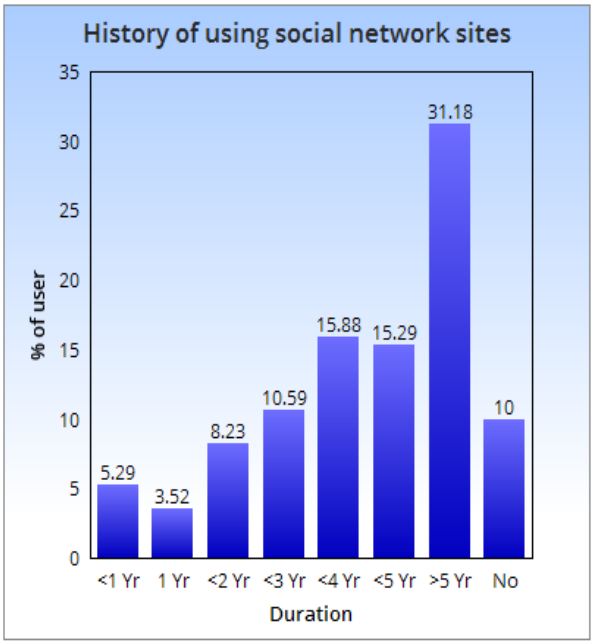

Fig 3: History of using social network sites- Duration

4.4 Users profile name

According to come about, 83% clients have genuine name on informal communication locales while 5% clients have fractional name and 2.35% clients have fake name.

4.5 Share contact details on social sites

The study result demonstrates that lion's share (68.82%) of the clients were not sharing individual points of interest on social destinations.

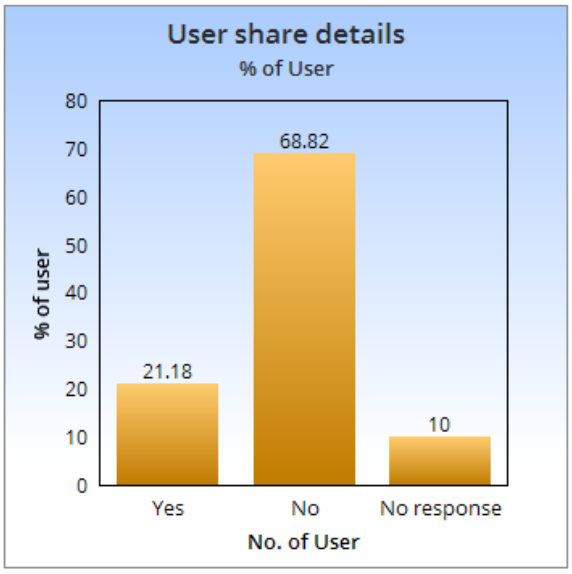

Fig 4: user share contact detail on social network

4.6 Users satisfied with privacy setting

The outcome demonstrates that 23% clients were not happy with protection setting of social destinations and 77% clients were happy with the default security setting anyway they likewise expressed that default protection setting required change.

4.7 Usertrusts the privacy setting and share photographs on Facebook

The outcome demonstrates that 41% clients did not trust security setting of social destinations and 49% clients believed the Facebook security setting while 10% of the clients did not reaction. Due to their trust, they share photos and 49% client share photos. Very nearly 75% of clients don't read the security arrangement and perhaps that is the reason that of them doesn't believe the Social systems administration destinations supplier in ensuring their own data.

4.8 User experienced privacy breach and identity theft

Still 25% individuals have encountered protection rupture and fraud in person to person communication locales and 10% client did not reaction. An information about their data fraud among them, 31% client replied in yes.

4.9 Default privacy setting of Facebook need improvement

About 85% users want improvement in default privacy setting of Facebook. And 84.7% users said there are many scope of improvement in security setting of Facebook.

Table 1. Default privacy setting of Facebook need improvement

Response	No. of users	% of users
Yes	145	85.29
No	17	10
Depends	8	4.70
Total	170	100

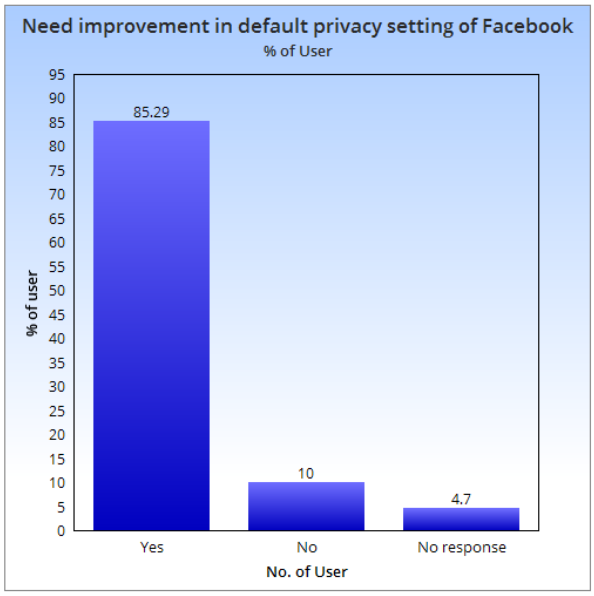

Fig 5: Default privacy setting of Facebook need improvement

5. ACKNOWLEDGMENTS

We are grateful to Dr. Vinita Gaikwad, Director (TIMSCDR) who was a constant source of help and played an important role during the development of this researchpaper.

6. REFERENCES

[1] Chewae`M., Hayikader`S., `Hasan`M`H. `and Ibrahim`J. 2015 How`Much`Privacy We Still Have on Social Network?. International Journal of Scientific and Research Publications, Volume 5, Issue 1, January 2015 Edition,page no:1.

[2] Adgaonkar`, A. `and Shaikh`, H. 2015 Privacy in Online Social Networks (OSNs). International Journal of Advanced Research inComputer Science and Software Engineering, Volume 5, Issue 3, March 2015.

[3] Ananthula S., Abuzaghleh'O. BharathiAlla'N. Chaganti'S.P., Pragnachowdarykaja'p. andMogilineedi D. 2015. measuring' privacy in online social networks. International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 2, May 2015.

[4] Gross R and Acquits A. Information revelation and privacy in online social netwoks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 2005, pp. 71–80.

[5] Srivastava A. and Geethakumari G. 2013 Measuring Privacy Leaks in Online Social Networks, International Conference on Advances in Computing,Communications and Informatics (ICACCI), pp. 2095-2100, 2013.

[6] Srivastava A and Geethakumari G. A Framework to Customize Privacy Settings of Online Social Network Users. 2014 IEEE Recent Advances in Intelligent Computational Systems (RAICS), pp. 187-192, 2013.

[7] Gangopadhyay S and Dhar M. D. social networking sites and privacy issues concerning youths. Article – 2 Global Media Journal-Indian Edition Sponsored by the University of Calcutta/www.caluniv.ac.in ISSN 2249 – 5835 Summer Issue/June 2014/Vol. 5/No. 1.

[8] Gunatilaka D. A Survey Of Privacy And Security IssuesInSocialNetwork.http://www.cse.wustl.edu/~jain/cse571-11/ftp/social/index.html.

[9] Pesce and Casas Privacy Attacks in Social Media Using Photo Tagging Networks: A Case Study with Facebook

[10] D. Boydand E.Hargittai. 2010. Facebook privacy settings:Who cares?" Journal on the Internet, 15(8), 2010.